UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/623,296	07/18/2003	W. Keith Edwards	PARC-DA3285	4686

22835 7590 01/29/2007
PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER	
LOVING, JARIC E	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/623,296	EDWARDS ET AL.	
	Examiner	Art Unit	
	Jaric Loving	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 November 1306*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-16,18-27 and 29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-16,18-27 and 29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is responsive to Applicant's amendment received on November 13, 2006. Claims 1-5, 7-16, 18-27, and 29-33 are pending. Claims 6, 17, and 28 have been cancelled.

2. Applicant's arguments filed on November 13, 2006 have been fully considered, but they are not persuasive.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Ramanathan, US 6,948,060.

In claim 1, Ramanathan discloses a system comprising:

a controller module comprising instructions for controlling a first component (col. 2, lines 34-48; col. 3, lines 1-7 – server controls network element); and

a second component with a security system that interacts with the controller module to implement a security protocol before a second component can control the first component based on executing the instructions in the controller module, wherein

the controller module provides secure control of communication between the first component and the second component, and wherein the security system decrypts an encrypted controller module to perform a portion of the security protocol, the second component controls the first component based upon the execution of the instructions in the controller module (col. 2, lines 34-48; col. 3, lines 1-17; col. 4, line 55 – col. 5, line 4; col. 5, lines 8-33).

In claim 2, Ramanathan discloses the system as set forth in claim 1 wherein a portion of the instructions in the controller module comprises authentication instructions which when executed by the second component cause the second component to send authentication information to the first component to perform a portion of the security protocol (col. 3, lines 18-27 and lines 50-61; col. 4, lines 29-45).

In claim 3, Ramanathan discloses the system as set forth in claim 2 wherein the authentication information is associated with an operator of the second component, the first component authenticates the operator using the authentication information to perform another portion of the security protocol (col. 3, lines 7-27 and lines 50-61; col. 4, lines 29-45).

In claim 4, Ramanthan discloses the system as set forth in claim 2 wherein the first component authenticates the second component using the authentication information to perform another portion of the security protocol, wherein upon unsuccessful authentication the first component rejects messages from the second component and upon successful authentication the first component accepts the messages from the second component, the messages being associated with controlling

the first component (col. 3, lines 7-27; col. 4, lines 29-55 – if not authorized, then no communication permitted).

In claim 5, Ramanathan discloses the system as set forth in claim 2 wherein the first component authenticates each of a plurality of messages received from the second component, the messages being associated with controlling the first component, wherein upon unsuccessful authentication of at least one of the messages the first component rejects the at least one message and upon successful authentication of another at least one of the messages the first component accepts the other at least one message from the second component (col. 4, line 55 – col. 6, line 4).

In claim 7, Ramanathan discloses the system as set forth in claim 6 wherein the security system uses a cryptographic key associated with one of the first component, the second component and a third component to decrypt the encrypted controller module (col. 4, line 55 – col. 5, line 4; col. 5, lines 8-33).

In claim 8, Ramanathan discloses the system as set forth in claim 1 wherein the security system authenticates the controller module using at least one of a digital certificate, a public key and a shared secret to perform a portion of the security protocol (col. 3, lines 29-36).

In claim 9, Ramanathan discloses the system as set forth in claim 1 wherein the security system rejects the controller module upon determining that a cryptographic signature associated with the controller module is not associated with a trusted component to perform a portion of the security protocol (col. 3, lines 44-61; col. 4, lines 18-29).

In claim 10, Ramanathan discloses the system as set forth in claim 1 wherein the controller module is encrypted using a cryptographic key from one of the first component, the second component and a third component (col. 3, lines 29-36; col. 4, line 55 – col. 5, line 4).

In claim 11, Ramanathan discloses the system as set forth in claim 1 wherein the controller module comprises a cryptographic signature associated with at least one of the first component and one or more third components (col. 3, lines 29-36; col. 4, lines 18-29).

In claims 12 and 23, Ramanathan discloses a method and computer readable medium comprising:

providing a controller module comprising instructions for controlling a first component (col. 2, lines 34-48; col. 3, lines 1-7); and

interacting with the controller module to implement a security protocol before a second component can control the first component based on executing the instructions in the controller module, wherein the controller module provides secure control of communications between the first component and the second component (col. 2, lines 34-48; col. 3, lines 1-17),

wherein the interacting with the controller module to implement the security protocol further comprises:

decrypting an encrypted controller module to perform a portion of the security protocol (col. 4, line 55 – col. 5, line 4; col. 5, lines 8-33), and

controlling the first component based upon the execution of the instructions in the controller module (col. 4, line 55 – col. 5, line 4; col. 5, lines 8-33).

In claims 13 and 24, Ramanathan discloses the method and computer readable medium as set forth in claims 12 and 23, respectively, wherein the interacting with the controller module to implement the security protocol further comprising:

executing a portion of the instructions in the controller module that comprises authentication instructions (col. 3, lines 18-27 and lines 50-61; col. 4, lines 29-45);

sending authentication information from the second component to the first component to perform a portion of the security protocol based on the executed authentication instructions (col. 3, lines 18-27 and lines 50-61; col. 4, lines 29-45).

In claims 14 and 25, Ramanathan discloses the method and computer readable medium as set forth in claims 13 and 24, respectively, further comprising authenticating an operator of the second component using the authentication information to perform another portion of the security protocol (col. 3, lines 7-27 and lines 50-61; col. 4, lines 29-45).

In claims 15 and 26, Ramanathan discloses the method and computer readable medium as set forth in claims 13 and 24, respectively, further comprising:

authenticating the second component using the authentication information to perform another portion of the security protocol (col. 3, lines 7-27; col. 4, lines 29-55); and

rejecting messages from the second component upon unsuccessful authentication and accepting the messages from the second component upon

successful authentication, the messages associated with controlling the first component (col. 3, lines 7-27; col. 4, lines 29-55).

In claims 16 and 27, Ramanathan discloses the method and computer readable medium as set forth in claims 13 and 24, respectively, further comprising:

authenticating each of a plurality of messages from the second component, the messages associated with controlling the first component (col. 4, line 55 – col. 6, line 4); and

rejecting at least one of the messages from the second component upon unsuccessful authentication of the at least one message and accepting another at least one of the messages upon successful authentication of the other at least one message (col. 4, line 55 – col. 6, line 4).

In claims 18 and 29, Ramanathan discloses the method and computer readable medium as set forth in claims 17 and 28, respectively, further comprising using a cryptographic key associated with one of the first component, the second component and a third component to decrypt the encrypted controller module (col. 4, line 55 – col. 5, line 4; col. 5, lines 8-33).

In claims 19 and 30, Ramanathan discloses the method and computer readable medium as set forth in claims 12 and 23, respectively, further comprising authenticating the controller module using at least one of a digital certificate, a public key and a shared secret to perform a portion of the security protocol (col. 3, lines 29-36).

In claims 20 and 31, Ramanathan discloses the method and computer readable medium as set forth in claims 12 and 23, respectively, further comprising rejecting the

controller module upon determining that a cryptographic signature associated with the controller module is not associated with a trusted component to perform a portion of the security protocol (col. 3, lines 44-61; col. 4, lines 18-29).

In claims 21 and 32, Ramanathan discloses the method and computer readable medium as set forth in claims 12 and 23, respectively, further comprising encrypting the controller module using a cryptographic key from one of the first component, the second component and a third component (col. 3, lines 29-36; col. 4, line 55 – col. 5, line 4).

In claims 22 and 33, Ramanathan discloses the method and computer readable medium as set forth in claims 12 and 23, respectively, where the controller module comprises a cryptographic signature associated with at least one of the first component and one or more third components (col. 3, lines 29-36; col. 4, lines 18-29).

Response to Arguments

5. Regarding claims 1-5, 7-16, 18-27, and 29-33, Applicant basically argues Ramanathan is inapplicable to independent claims 1, 12, and 23 and therefore, the remaining dependent claims are allowable.

As to claims 1, 12, and 23, Applicant argues "[t]here is nothing within Ramanathan, either explicit or implicit, which suggests securely controlling communications between a first component and a second component. Examiner contends Ramanathan discloses this limitation. In paragraph [0004] of Applicant's specification, Applicant states "... a second component can control the first component based on executing the instructions in the controller module." Further, in paragraph [0034] of Applicant's specification, Applicant states "The server controller object 22(1)

includes mobile code instructions... to generate custom user interfaces..." In col. 2, lines 34-48, Ramanathan states that a policy server utilizes a network use digital contract in accordance with a network policy. In col. 3, lines 1-10, Ramanathan describes the network policy (NP) as being "defined, distributed and administered by policy administrator." Ramanathan further states "[a] network element may only communicate with another network element in accordance with a particular communication rule defined in the NP." Therefore, the policy rules enforce control on network elements through the policy server, similar to a second component controlling the first component based on executing instructions in the controller module.

The remaining dependent claims follow the reasoning of the independent claims.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jaric Loving whose telephone number is (571) 272-1686. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JL

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER